DEPARTMENT OF THE NAVY
NAVAL SCHOOL OF HEALTH SCIENCES
BETHESDA MARYLAND 20889-5611

IN REPLY REFER TO:
NSHSBETHINST 5510.1L
Code 0S
14 NOV 2001

NSHS BETHESDA INSTRUCTION 5510.1L

From: Commanding Officer

Subj: SECURITY OF CLASSIFIED INFORMATION

Ref: (a) SECNAVINST 5510.30A
(b) SECNAVINST 5510.36

Encl: 1 Procedures for Verifying Security Clearances and Granting Access for NSHS Personnel
(2) Security Clearance and Access Process Flowchart

1. **Purpose**. To outline procedures for the receipt, control disclosure and destruction of classified material at this Command.

2. **Cancellation**. NSHSBETHINST 5510.1K

3. **Applicability**. This regulation applies to all military, civilian, and contract members of the Naval School of Health Sciences (NSHS), Bethesda or those serving in an advisory/ consultant capacity to NSHS whether on a permanent, temporary, or part-time basis. Every person in the Department of the Navy having access to classified material is responsible for safeguarding that material at all times against loss or compromise. Personnel holding a security clearance at this Command should be familiar with the general regulations governing the security of classified material as set forth in reference (a), and with this instruction, which provides control procedures.

4. Security Organization

a. Security Manager - The Security Manager position will be designated in writing by the Commanding Officer as a collateral duty. The Security Manager shall be the principal advisor on information and personnel security in the Command.

b. Assistant Security Manager - The Assistant Security Manager(s) will be assigned in writing by the Commanding Officer. The Assistant Security Manager(s) are to support the

Security Manager in the administration of security programs. The Assistant Security Manager will assume the classified material control function in an emergency or during the absence of the Security Manager.

c. Security Assistant - Security Assistant(s) may be assigned as needed for administrative functions under the direction of the Security Manager. Security Assistants shall only be assigned to assist on issues for which they have the required clearance and access.

d. Information Systems Security Manager (ISSM) - The ISSM is responsible to the Commanding Officer to develop, maintain, and direct the implementation of the Information Security (INFOSEC) Pgram within the Command. The ISSM advises the Commanding Officer on all INFOSEC matters and serves as the Command's point of contact for all INFOSEC issues.

5. **Classified Material Control Program**. Safeguarding of classified material, including registered and technical publications, is accomplished through centralized control by the Security Manager. The Security Manager, or assistant, is responsible to the Commanding Officer for the receipt, custody, control and destruction of classified material.

6. **Receipt of Classified Material**. Normally, the Security Manager will receive all incoming classified material, prepare necessary receipt and control records, and deliver the classified material to the Executive Officer and the Commanding Officer for review. In the temporary absence of the Security Manager, classified material will be received and held or forwarded by the designated alternate. If classified messages are received outside of normal working hours, the Officer of the Day (OOD) will notify the Security Manager that classified material addressed to NSHS is available at the National Naval Medical Center's message center. The Security Manager will assist the OOD in taking required action and secure the material. In the absence of the Security Manager, the OOD will notify a designated alternate.

7. **Control of Classified Material**. The Security Manager will maintain physical custody or inventory control of all classified material. The Security Manager will only release classified material to personnel who have the appropriate clearance (interim or final) and a need to know. All security clearances must be documented on OPNAV Form 5520/20. Access to classified material is controlled and granted by the Security Manager on a

need to know basis. Enclosure (1) provides procedures used by the Security Manager to grant personnel access to classified material. Personnel who have temporary custody of classified material will return the material to the Security Manager at the end of working hours daily. The classified material safe shall be secured at all times when unattended. An inventory board of two commissioned officers will be appointed in writing by the Commanding Officer to inventory classified material at the Naval School of Health Sciences, Bethesda, Maryland. This Board shall conduct a biannual inventory of classified material and make a report to the Commanding Officer of their findings.

8. **Disclosure of Classified Material**. All personnel receiving or holding classified material will ensure that disclosure of the contents to others is based on appropriate security clearance and a demonstrated "need to know". Further, they will ensure that classified material is physically safeguarded at all times, and that classified material is removed from the Command only as authorized by the Commanding Officer and in strict accordance with procedures outlined in reference (a). In the event that a violation of any of the above requirements is discovered, the person making the discovery will protect the classified material, and immediately notify the Security Manager or the Commanding Officer.

9. Security Containers

a. Only security containers authorized by reference (a) will be used to store classified material.

b The following procedures shall apply:

(1) Combinations will be known only to those whose official duties demand access to the container involved.

(2) The combination will be changed at least annually. It is also required to change the combination whenever the Security Manager, Assistant Security Manager, or any individual who knows the safe combination transfers or is removed from the position of trust. The combination is also to be changed whenever there is a reason to believe that the security container has been compromised.

(3) In selecting combination numbers, multiples of 5's, simple arithmetical series, and personal data such as birth dates and serial numbers should be avoided.

(4) All personnel with access to the security container will demonstrate the practice of securing the container by rotating the dial of the combination lock at least four complete turns in the same direction and checking to ensure that the container is secure.

(5) Security checks should be performed and documented on the Activity Security Checklist (SF 701), as required by reference (a).

10. **Destruction of Classified Material**. Classified material will be destroyed by burning, shredding or other means as prescribed in reference (a).

a. Routine Destruction. At least annually, the Security Manager will review classified materials, identify those items of no functional or historical value which are authorized for destruction in accordance with reference (a), and present a proposed destruction list to the Executive Officer for approval Destruction will be accomplished as follows:

(1) Top Secret: Security Manager and two witnesses cleared to Top Secret.

(2) Secret and below: Security Manager and one witness cleared to the level of the material being destroyed.

(3) The destruction of Top Secret and Secret material will be recorded on OPNAV 5511/12 (Classified Material Destruction) and records will be maintained for 2 years.

b. Emergency Destruction. In the event of war or disaster, if the probability of compromise of classified material appears imminent, the Security Manager or alternate shall, upon approval of the Commanding Officer, destroy all classified material in the following order:

(1) Top Secret (including Registered and Technical publications)

(2) Secret

(3) Confidential

11. **Security Education**. Security training, as well as all staff training, is conducted through the Academic Directorate. The Security Manager is responsible for assisting with topic and

lesson plan development. General security training is provided to all NSHS personnel during Command orientation. Either topical or focused training may be provided to all or certain sections of the staff periodically as appropriate. Additional annual refresher training is provided to Command members with access to classified information.

12. **Reporting Security Compromises**

a. Reference (b) provides procedural guidance to follow in the event of security compromises. A security compromise is defined as the unauthorized disclosure of classified information to a person(s) who does not have a valid clearance, authorized access, or a need-to-know. Any individual who becomes aware that classified information is lost or compromised shall immediately notify the Commanding Officer or Security Manager. If it is believed that the Commanding Officer or Security Manager may be involved in the incident or notification is impractical, the individual may notify the Security Manager at the Bureau of Medicine and Surgery, Naval District Washington, or contact the local Naval Criminal Investigative Service office.

b. Upon notification of loss or compromise of classified information, the Commanding Officer shall immediately notify the local NCIS office and initiate a Preliminary Inquiry.

c. All personnel are reminded to remain security conscious and to always be mindful of suspicious behavior or unusual circumstances that may represent security concerns. Individuals are to report any such behavior to the Security Manager. We all have the responsibility to uphold our duty and safeguard any sensitive information with which we are entrusted.

D. S. WADE

Distribution:
Lists I and III

Procedures for Verifying Security Clearances and Granting Access for NSHS Personnel

1. This is a guide for verifying security clearances and granting access for all NSHS Bethesda personnel. These procedures will normally be accomplished when a person checks on board the Command. They also will apply to personnel currently on board who require verification of their security clearance and access to classified documents to perform their duties.

2. A security clearance denotes only that an individual is eligible for access, it does not authorize access. Access to classified material within the Command will be granted only when all of the following conditions have been met:

a. The individual concerned possesses a valid security clearance.

b. The individual concerned has been properly counseled on the responsibilities for handling classified material.

c. The individual concerned has been determined to have an official "need to know".

3. Procedures:

a. The Security Manager will:

(1) Conduct an orientation briefing for all newly reporting personnel. This briefing will consist of:

(a) Command procedures for handling and storage of classified documents within the command.

(b) Procedures for transporting classified material to/from the command.

(c) Procedures for receipt of classified materials from outside the command.

(2) Perform a local records review to include whenever possible:

Health Record

Dental Record

(c) Personnel (Service) Record

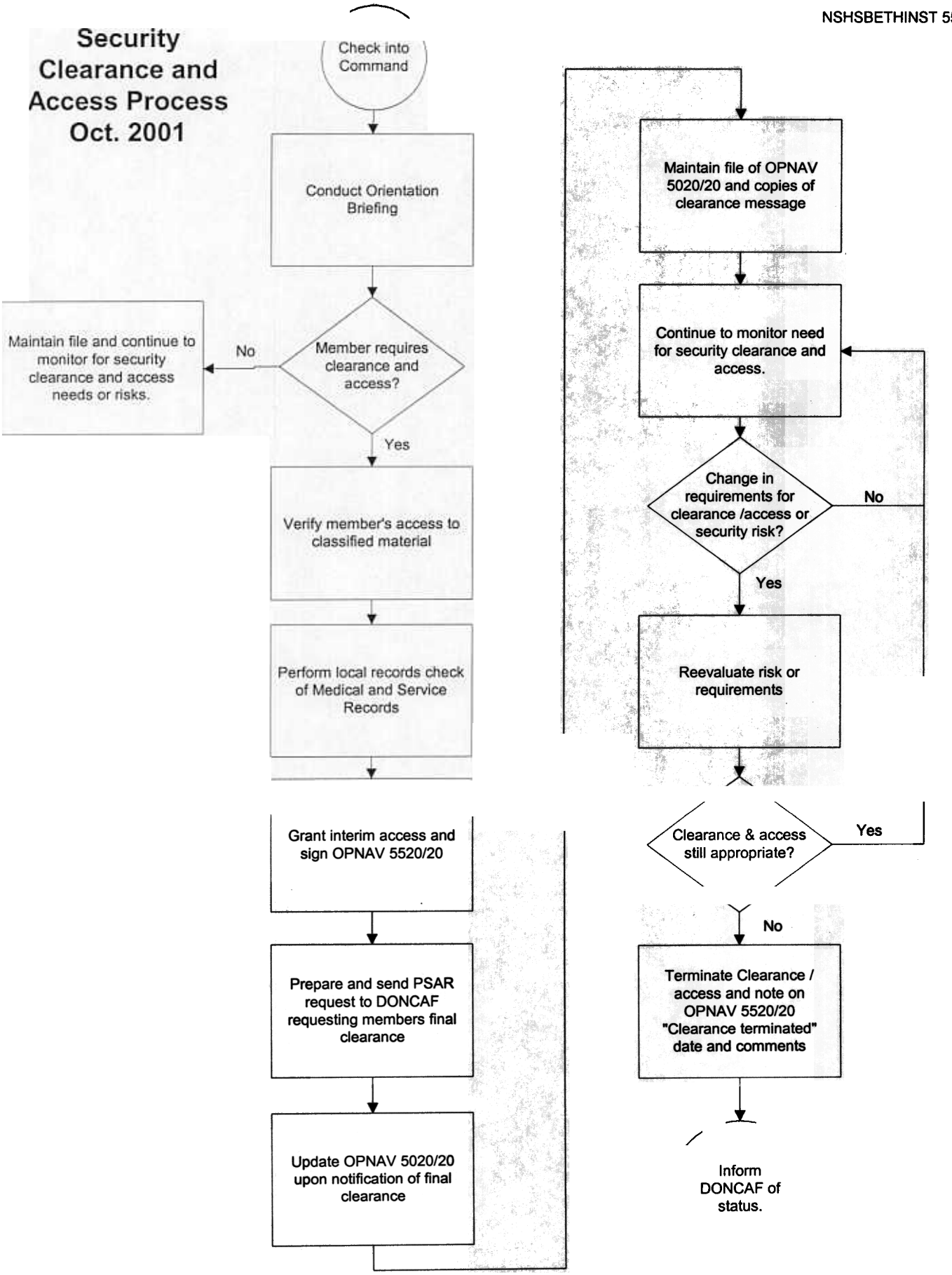
(3) Grant interim access by signing OPNAV 5520/20

(4) Prepare and send by either fax or mail, the Personnel Security Action Request (OPNAV 5510/413) for submission to DONCAF requesting the member's final clearance. If an initial request for a clearance or a periodic reinvestigation is required, it will be processed using the Electronic Personnel Security Questionnaire Program.

(5) When notification of final clearance is received, update the OPNAV 5520/20. If needed, have member sign Nondisclosure agreement (SF 312). Document on OPNAV 5520/20 in the comment section "SF-312 executed this date" if member signs SF-312.

(6) Maintain a file on all personnel with clearances and access. Copy of message from DONCAF is to be kept on file with members completed OPNAV 5520/20 until member's PCS or transfer.

4. Eligibility for access to classified material must be continuously evaluated by supervisory personnel. If at any time an individual fails to meet the criteria set forth in reference (a), the individual's access to classified material will be terminated immediately, noting on OPNAV 5520/20 in the comment section as to why clearance was terminated. The Security Manager shall ensure that DONCAF is properly notified of all information relative to an individual's ability to hold a clearance and have access, using the Personnel Security Action Request (OPNAV 5510/413).


Security Clearance and Access Process Oct. 2001
Check into Command
Conduct Orientation Briefing
Member requires clearance and access?
No
Maintain file and continue to monitor for security clearance and access needs or risks.
Yes
Verify member's access to classified material
Perform local records check of Medical and Service Records
Grant interim access and sign OPNAV 5520/20
Prepare and send PSAR request to DONCAF requesting members final clearance
Update OPNAV 5020/20 upon notification of final clearance
Maintain file of OPNAV 5020/20 and copies of clearance message
Continue to monitor need for security clearance and access.
Change in requirements for clearance /access or security risk?
No
Yes
Reevaluate risk or requirements
Clearance & access still appropriate?
Yes
No
Terminate Clearance / access and note on OPNAV 5520/20 "Clearance terminated" date and comments
Inform DONCAF of status.